NORTON ROSE FULBRIGHT

Preparing for the expected and the unexpected: The New York Department of Financial Services' Cybersecurity Regulation

While the sufficiency of cybersecurity programs was previously subject to "reasonableness" standards, an"acceptable" cybersecurity program has become more objective as regulators, such as NYDFS, continue to implement, amend and mature applicable laws.

By Dan Pepper and Kate Nelson, *New York Law Journal* — March 01, 2024

When the first public data breach occurred in 2005, there was little to no legal oversight in place. In response to data breaches, the threat actors typically garnered the exclusive responsibility. As the law has evolved and data security incidents have become more common, public and regulatory sentiment has shifted from blaming the threat actor toward holding the victim company accountable based on its purportedly deficient cybersecurity program.

While the sufficiency of these programs were previously subject to subjective "reasonableness" standards, an"acceptable" cybersecurity program has become more objective as regulators, such as the New York Department of Financial Services (NYDFS), continue to implement, amend and mature applicable laws, laying out clear standards and expectations as described below.

Overview of the cybersecurity regulation

On Nov. 1, 2023, NYDFS announced the final amendments to 23 NYCRR Part 500 (Cybersecurity Regulation),implementing various mandates that go into effect over the next two years.

The first requirements went into effect Dec. 1, 2023 and include new data breach reporting obligations. First, covered entities are required to notify the NYDFS within 72-hours of determining that a ransomware incident has impacted a material part of the entity's information system (including ransomware incidents at affiliates and third-party service providers). Second, regardless of the impact to the victim's information system, the new regulations also require notification to the NYDFS within 24-hours whenever an extortion payment is made.

Additional requirements such as mandated cybersecurity policies, plans and procedures; technical and governance requirements; and annual compliance certification obligations go into effect at various times between April 15, 2024, and Nov. 1, 2025. The NYDFS has provided a detailed timeline for covered entities.

Recent enforcement actions and settlements

The NYDFS is far from inexperienced when it comes to the cybersecurity and data privacy landscape. In fact, since first publishing its Cybersecurity Regulation in 2017 (which went into effect March 2019), the NYDFS has been one of the most active regulators in the financial industry, particularly when it comes to cybersecurity. In recent years, we have seen the NYDFS enter into consent orders with some of the largest penalties against companies for cybersecurity violations, and

Dan Pepper is a partner at Norton Rose Fulbright US, where he advises clients on proactive data privacy and security practices, data breach incident response and regulatory compliance. Kate Nelson is an associate at Norton Rose Fulbright US, where she advises clients on data breach incident response and regulatory compliance.

we do not expect this trend to abate, especially in light of the new requirements.

Recently, the NYDFS reached a settlement with Genesis Global Trading Inc. (GGT) for $8 million due to violations including non-compliance with the Cybersecurity Regulation. The consent order, dated Jan. 3, 2024, listed various deficiencies, including insufficient business continuity and disaster recovery (BCDR) procedures to address cybersecurity requirements; inadequate risk assessment that did not "allow for revision of controls to respond to technological developments and evolving threats" and did not adequately consider the cybersecurity risks to GGT's business operations"; and an inadequate incident response policy which did not include cybersecurity incident reporting obligations to the NYDFS.

Although the majority of the new rules are not yet enforceable, most of the cited failures and deficiencies are in line with the new rules (for example, new BCDR requirements described below).

What to expect in 2024

Resiliency has been a topic of interest from many regulators in response to data breaches lately. To no surprise, the new regulations also require that a covered entity's cybersecurity program addresses BCDR. We anticipate that the NYDFS will not only inquire about disruptions directly to the financial institution itself, but also about the level of impact to customers, advisors, partners, and other external stakeholders.

The NYDFS may scrutinize entities that are shut down for an unreasonable amount of time following a cybersecurity incident. What is reasonable will depend on the severity of the incident. For example, the BCDR plan should include restoring data from backups for critical services; however, threat actors often encrypt backups as well.

Another significant change to the Cyber security Regulation pertains to the roles and responsibilities of the chief information security officer (CISO). Particularly, the CISO must report to its company's senior governing body on material cybersecurity issues and file an annual notice of compliance with the NYDFS, in coordination with the highest-ranking company executive. Accordingly, it is important that cyber risk is communicated efficiently so that the appropriate people in the organization are adequately informed to make decisions.

Under the new rules, covered entities are required to annually conduct penetration tests, risk assessments and cybersecurity training, which must include awareness around social engineering tactics. While many covered entities already align with these requirements under cybersecurity standards such as the NIST Cybersecurity Framework,companies are encouraged to evidence compliance with these processes through the maintenance of comprehensive documentation.

It is also important to note that the cybersecurity training requirement explicitly calls out social engineering. These types of attacks have become more and more common and sophisticated. If an entity suffers an attack due to social engineering and such training was not comprehensive or enforced, the entity may face fines for noncompliance.

In the event of an investigation by the NYDFS, the superintendent will likely request copies of past penetration tests, risk assessments, and records of cybersecurity trainings, including lists of attendees. Accordingly, entities should consider the pros and cons of engaging external third parties to conduct assessments at the direction of outside legal counsel, in anticipation of litigation or regulatory investigations, to maintain attorney-client privilege over findings.

While the NYDFS may not uphold the privilege, finding that an engagement under outside counsel's direction amounts to trying to paper over a business as usual engagement, there are still other benefits to conducting these assessments under privilege. For example, significant findings of deficiencies, and remediation or mitigation measures taken in response, need to be carefully documented identifying accountable individuals or business units. Failure to remediate gaps or deficiencies may result in fines—for example, the GGT consent order also noted GGT's failure to address vulnerabilities identified in prior audits.

As mentioned above, any material risks or changes to the cyber program resulting from assessments such as penetration tests and risk assessments must be adequately relayed to the senior governing body or senior officer(s). A covered entity's legal department should play a key role in reporting those findings to executive leadership.

How can my company prepare?

We recommend that covered entities incorporate these new reporting requirements into their cybersecurity incident response plan(s) and consider creating a ransomware and cyber extortion playbook that specifies when notice is required, how such notice should be submitted, and who is responsible for such notice. The legal department should play a critical role in this process. In the event that a payment is made, and in anticipation of follow-up inquiries from the NYDFS, the playbook should also layout who within the company has the authority to approve a ransom/extortion payment, and the process to ensure compliance of such payment.

As with all policies and procedures, however, just documenting the process is not enough. It is important to train stakeholders and regularly test these processes, and indeed, the new rules also require exercises at least annually. Quick activation and regular testing of an efficient BCDR plan, including practical workarounds and availability of backups, is important to defend the reasonableness of disruptions resulting from a cybersecurity incident and reduce the likelihood of regulatory enforcement action.

Looking ahead to 2024 and beyond, the Cybersecurity Regulation is clear that a single act prohibited by Part 500, or the failure to satisfy an obligation, constitutes a violation. The NYDFS will consider mitigating factors when assessing penalties, such as good faith, history of prior violations, extent of harm to customers, gravity of violations, number of violations and length of time over which they occurred, and penalties or sanctions imposed by other regulators.

We anticipate that investigations by the NYDFS under the new rules will likely arise under two occasions: (1) if the CISO is unable to certify annual compliance and/or (2) if the entity fails to notify NYDFS within 72-hours of determining a ransomware incident impacts a material part of the entity's information systems. Due to the ambiguity of what constitutes a "material part of the entity's information system", we expect companies to struggle with making such a determination within this short time frame. To prepare, companies may want to proactively identify material information systems or create a procedure on how the entity will determine when a ransomware incident has a material impact.

Although some of the new requirements are not technically enforceable yet, the NYDFS likely expects companies to at least start taking reasonable measures (planning, budgeting and executing) to ensure compliance with these requirements.

For example, the NYDFS brought its first enforcement action under the Cybersecurity Regulation in 2020 against First American Title Insurance Company. Although the Cybersecurity Regulation did not go into effect until March 2019, the enforcement action cited security failures at First American as early as October 2014. Accordingly, we encourage covered entities to start reviewing and amending their cybersecurity processes and procedures now.

Some best practices to mature a covered entity's cyber program and comply with the requirements include:

- Conducting independent audits of the cybersecurity program based on risk assessment(s);
- Reviewing the current organizational governance and reporting structure to ensure that information security departments are reporting to senior management in a manner to effectively communicate and manage risks;
- Enhancing and enforcing security awareness and education training for employees, focusing on social engineeringand phishing and including active learning modules into the training;
- Implementing a privileged access management solution;
- Deploying an endpoint detection and response solution; and
- Implementing a managed detection and response service to detect unauthorized activity.